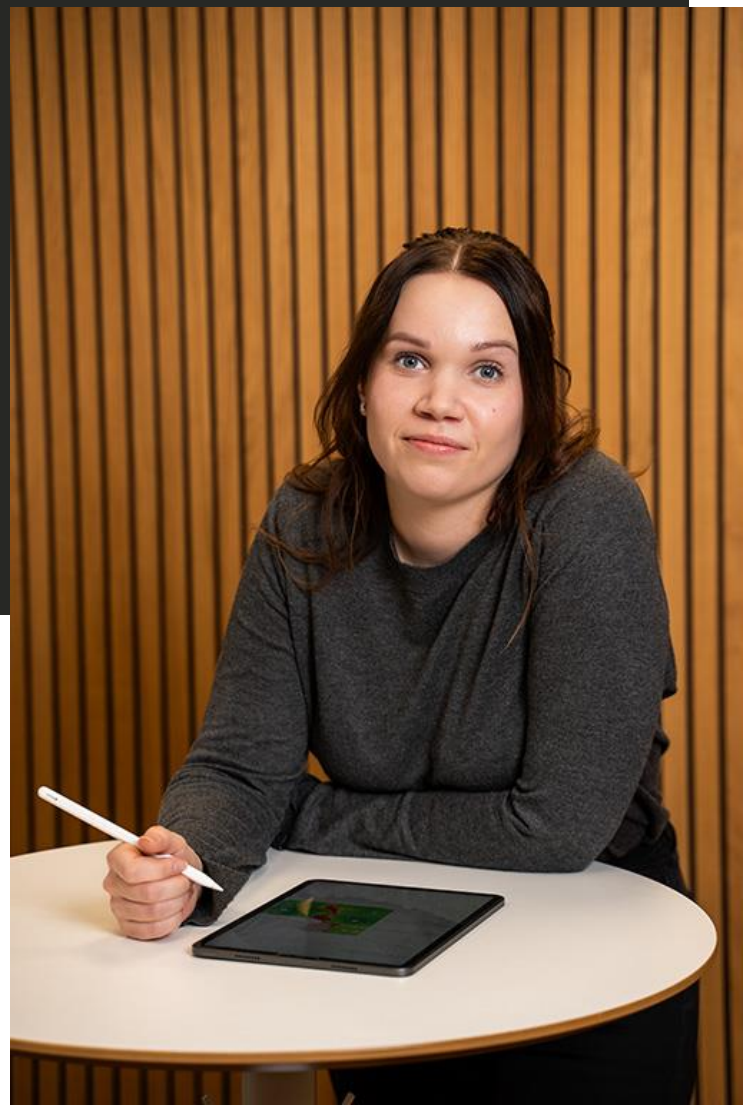
DataEnter

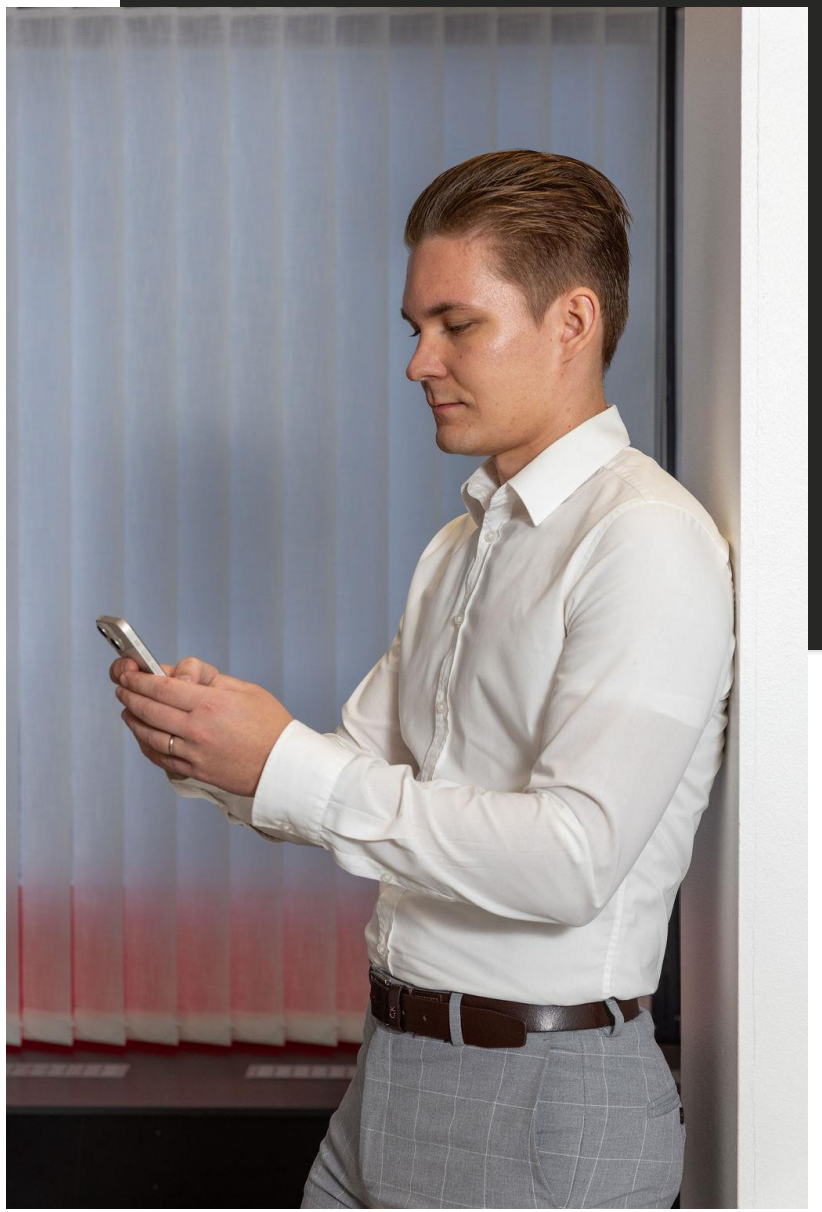


Operaatio datapanssari:

Käytännön keinoja Microsoft 365 - ympäristön tietoturvan parantamiseen

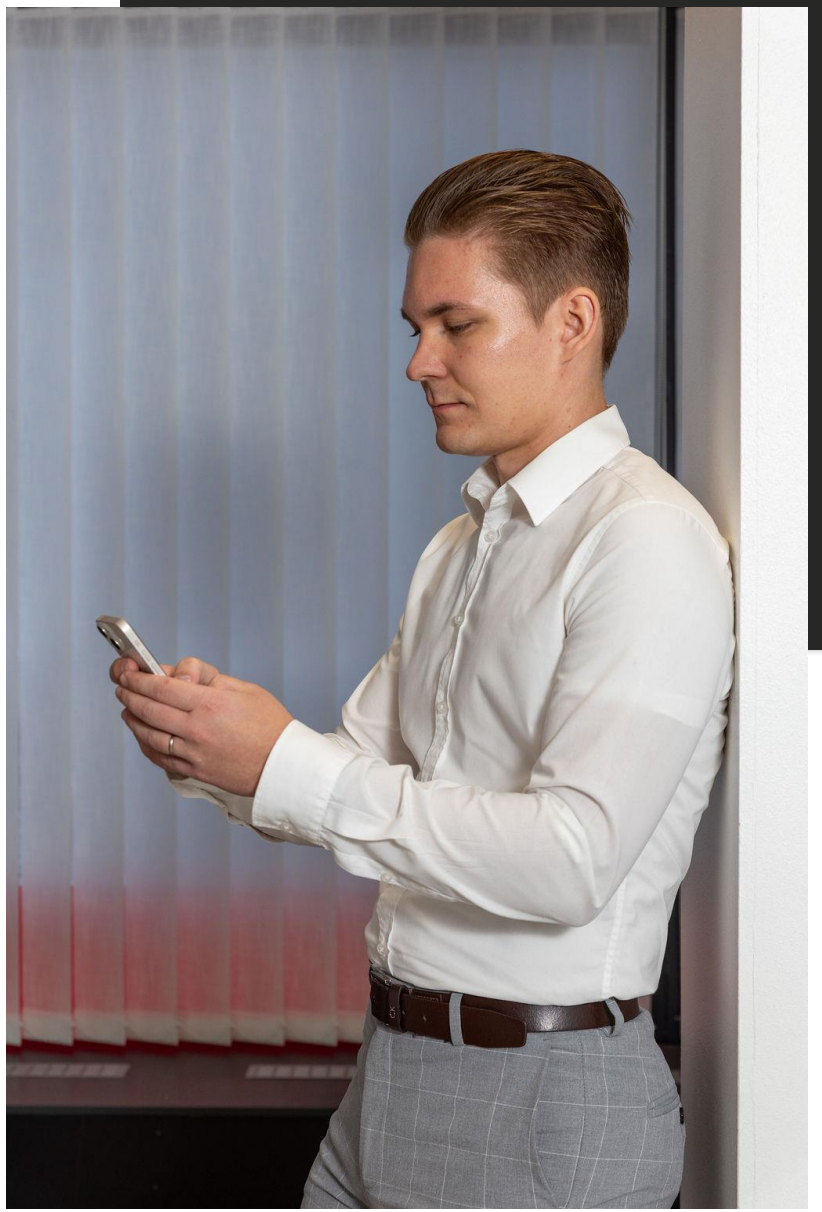
Toni Keränen

Miksi tietoturvaa pitää parantaa?



Miksi tietoturvaa pitää parantaa?

1) Maailma muuttuu
   NIS2- ja CER-direktiivit, Kyberturvallisuuslaki yms.
2) Järjestelmät muuttuvat
   Microsoft 365 change is constant, surprises are optional
3) Käyttäjät pysyvät ennallaan
   ”Käyttäjävirheet olivat osallisena 95% tietoturvaloukkauksia vuonna 2024”, lähde: Mimecast: The State of Human Risk



Miten tietoturvaa pitää parantaa?

Miten tietoturvaa pitää parantaa?

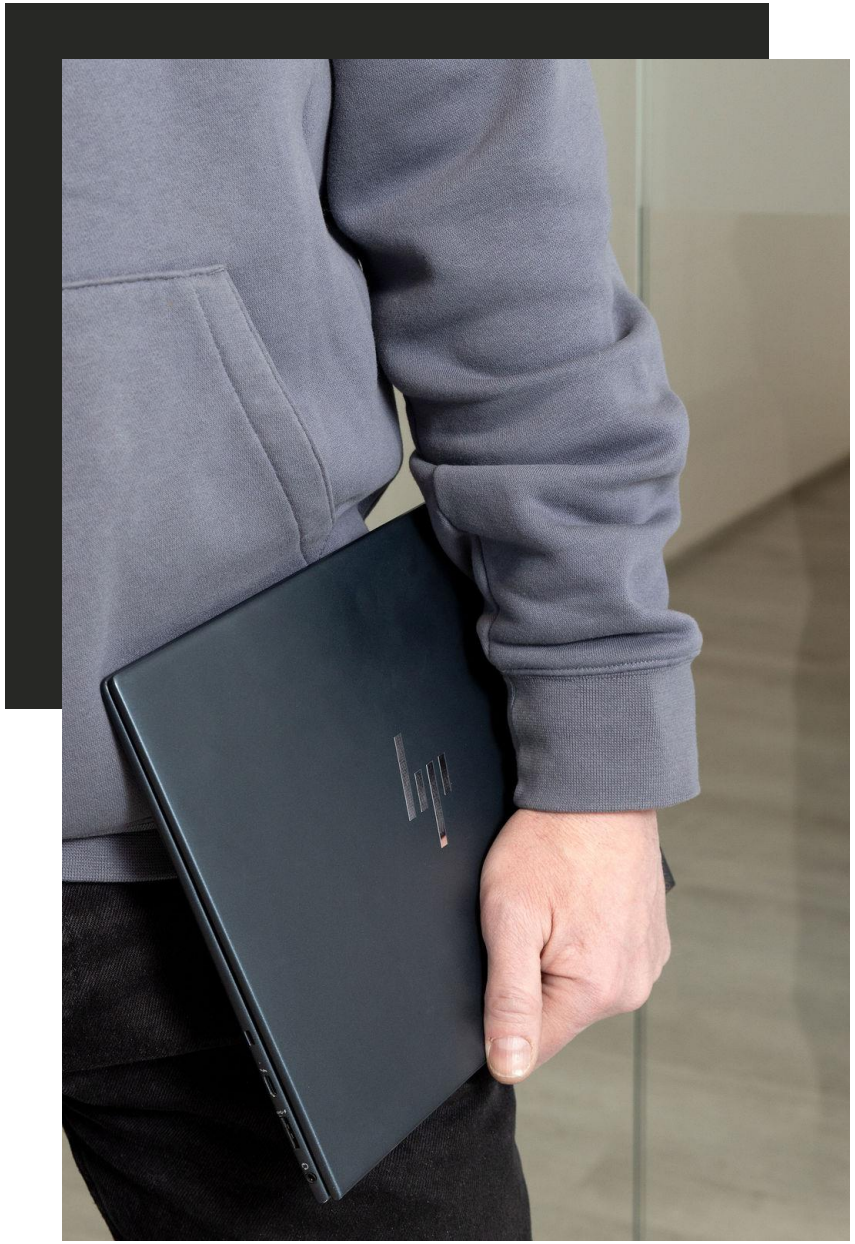
Kerroksittain ja pala kerrallaan.

Palaset:

1) Identiteetin hallinta
2) Pääsynhallinta
3) Päätelaitesuojaus
4) Tiedonsuojaus
5) Seurannan käyttöönotto
6) Hallinnointi ja prosessit

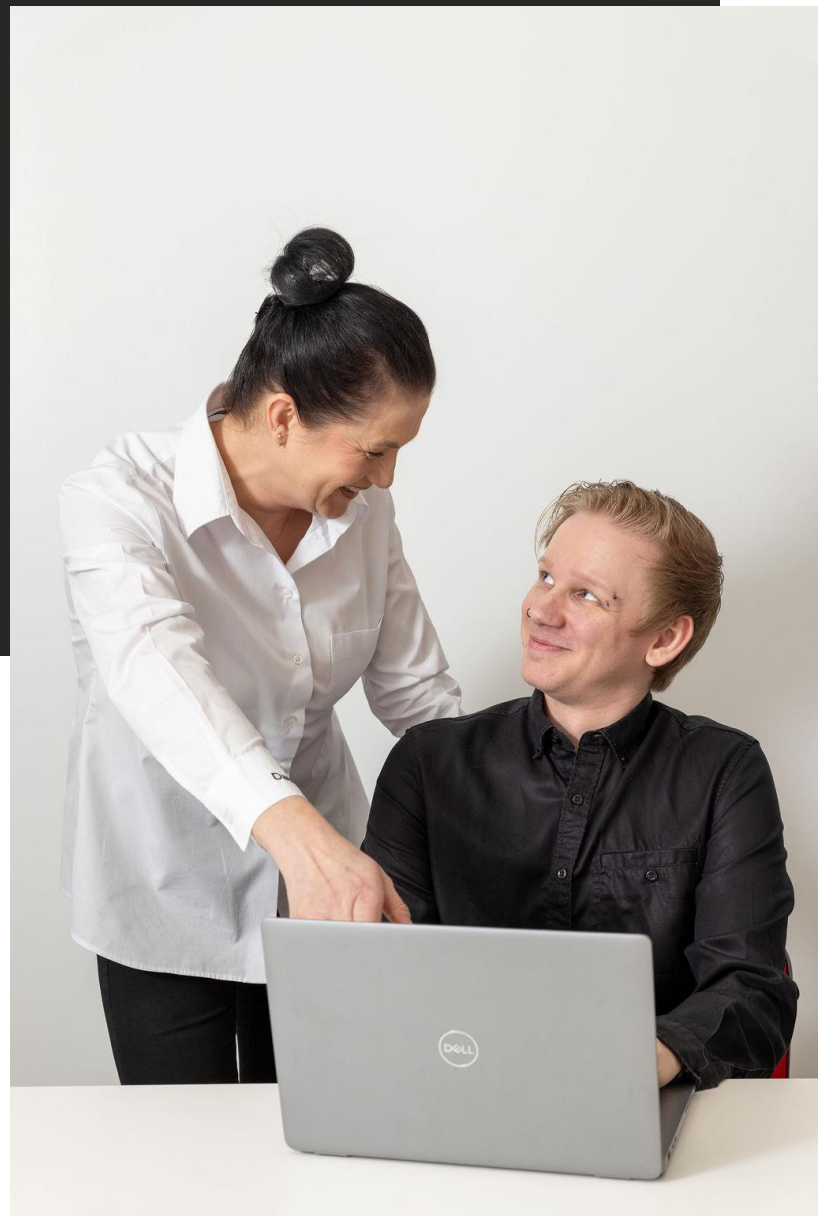
Monivaiheinen tunnistautuminen (MFA)

- Miksi monivaiheinen tunnistautuminen on tärkeää?
  - Salasanat vuotavat aina
  - Kalastelua, tietomurrot yms.
  - MFA katkaisee hyökkäyksen vaikka salasana olisi oikein
  - Estää arvioidusti ~99% automaattisista tilimurroista
- Miten?
  - Oletuksena päälle kaikille käyttäjille, ei pelkästään pääkäyttäjille
  - Käytä vahvoja tunnistautumismenetelmiä (SoftAuth / FIDO2 etc)
  - Vältä heikkoja (SMS / sähköposti)



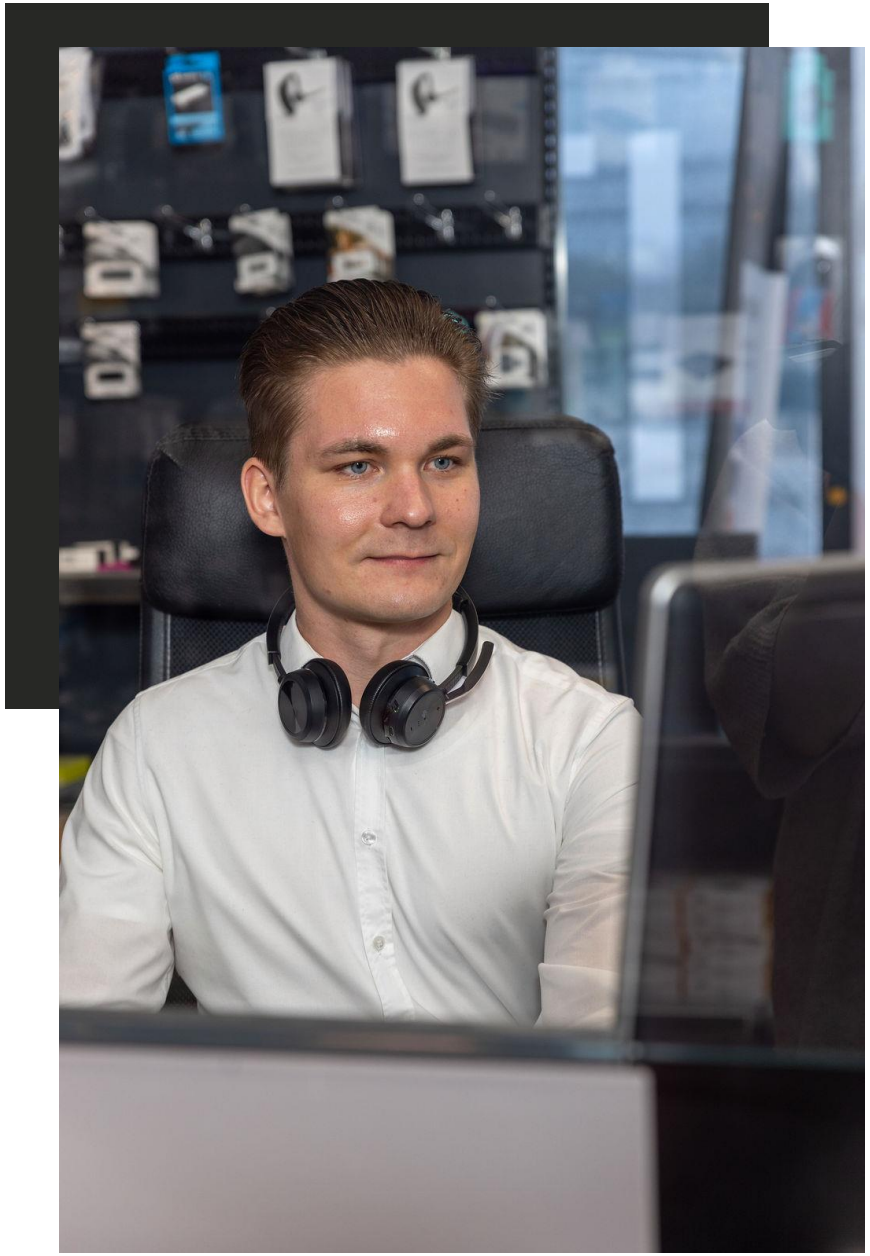
Salasanat

- Miksi salasanat ovat tärkeitä?
  - Salasanat vuotavat aina
    - Kalastelua, tietomurrot yms.
  - Käyttäjillä on tapana kierrättää salasanoja
- Miten?
  - Eri rooleille eri vaatimukset
    - Peruskäyttäjälle pitkä salasana ja vaihto harvoin, ellei koskaan,
      jos käytössä MFA.
    - Pääkäyttäjille pitkä salasana ja vaihto usein.
    - HUOM! Puhdas Entra ID -ympäristö ei tue salasanapoliitikoita.
  - Käyttöön kiellettyjen salasanojen listaukset
    - Esim. osat nimestä/käyttäjätunnuksesta tai organisaation nimestä.



Ehdollinen käyttöoikeus (CA)

- Miksi ehdolliset käyttöoikeudet ovat välttämättömiä?
  - Ilman niitä kaikilla laitteilla ja sovelluksilla on pääsy yrityksen 365-ympäristöön kaikkialta.
  - Kaikki käyttäjät ovat ns. samalla riskitasolla.
  - MS:n oletus asetukset eivät riitä
    - Ei roolikohtaisia sääntöjä, laite- tai selainvaatimuksia
- Miten?
  - Estetään vanhat autentikointitavat (ns. legacy authentication)
  - Estetään riskimaat
    - Suojataan salasanat ja tunnukset että pääsy riskimaista, pienentäen hyökkäys mahdollisuuksia massiivisesti.
  - Erotetaan käyttäjä- ja palvelu- sekä pääkäyttäjätilit toisistaan
    - Tiukemmat ehdot pääkäyttäjille



Vähimpien käyttöoikeuksien kulttuuri

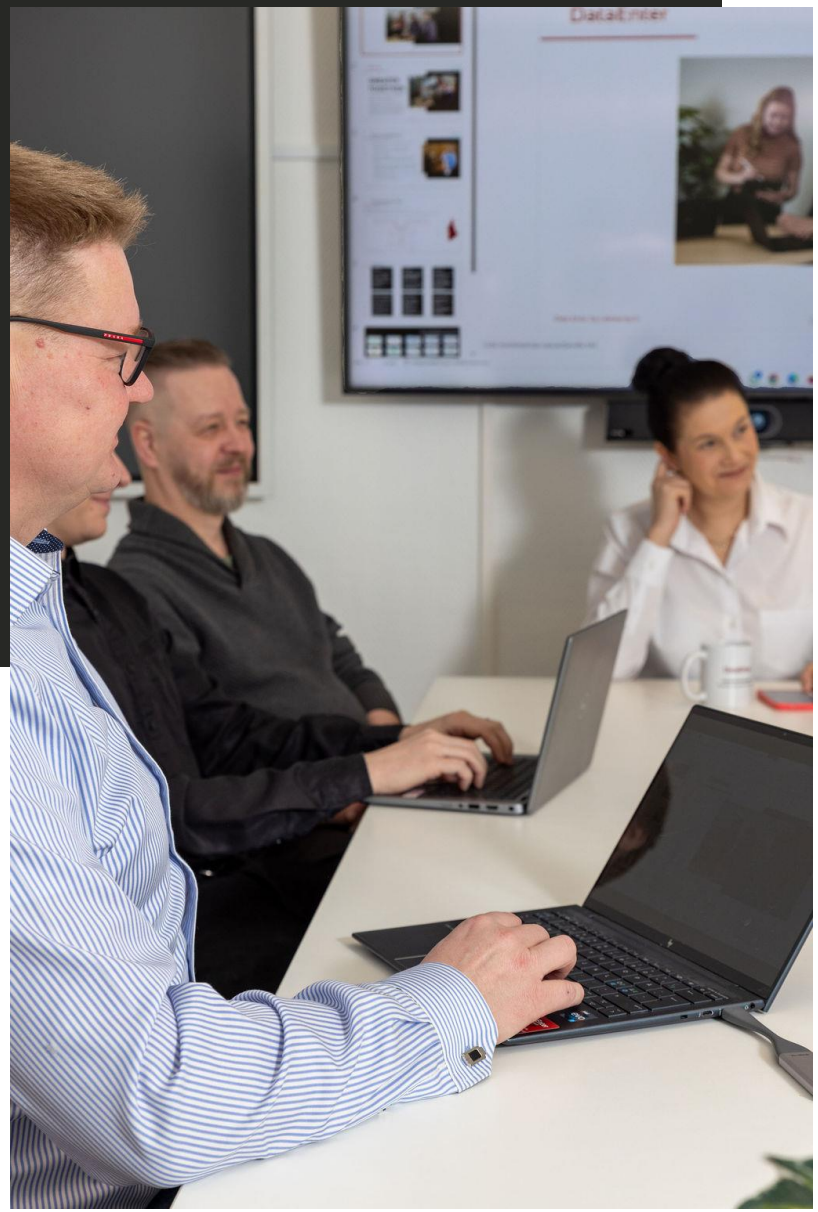
- Miksi pysyvät, liiat oikeudet ovat vaarallisia?
  - Jos tilille päästään, hyökkääjällä on heti hallussa kaikki
- Miten?
  - Annetaan oikeudet vain tarvittaessa
  - Pyynnöt jättävät seurantajäljen
    - Pyytäjä → Hyväksyntä (vaikka automaattinen) → Tietojen tallennus
  - Oikeudet roolien mukaan, ei ikinä käyttäjäkohtaisesti

Laitehallinta yrityksessä

- Miksi hallita yrityksen laitteita?
  - Tieto omasta omaisuudesta ja niiden tilasta
  - Keskitetystä hallinnasta voidaan tarkistaa että laitteet ovat turvallisia ja soveltuvia yrityksen käyttöön
  - Suojaudutaan uhkia vastaan laitetasolla
- Miten?
  - Yritystasolla määritetään laitevaatimukset
    - Laitteen salaus sekä muut turva ominaisuudet (Secure Boot + TPM)
    - Nykyaikainen virustorjunta (EDR) estää hyökkääjän liikkumisen myös sivuttain yrityksen sisällä.
    - Keskitetyt päivitykset takaavat että laitteet kaikilla samalla tasolla
      - Sopimattomilta laitteilta voidaan estä pääsy yrityksen 365-palveluihin
  - Ei henkilökohtaisia laitteita
    - Tuntematon ja hallitsematon laite = uhka.
  - Erota yrityksen tieto käyttäjien tiedoista
    - BYOD puhelimet

Sähköpostin suojaus yrityksessä

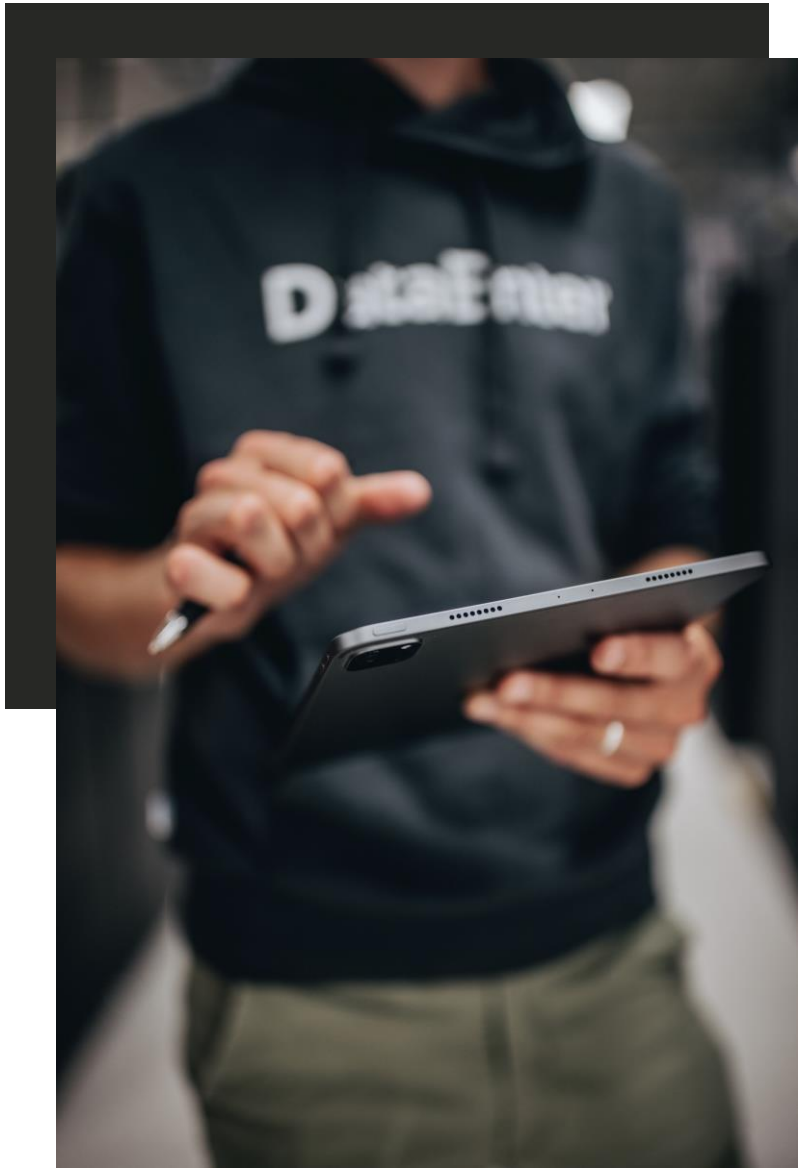
- Miksi suojata sähköposti?
  - Sähköposti on suurin yksittäinen hyökkäyskanava
  - Mahdollistaa myös tahattoman tietovuodon
- Miten?
  - Suojataan/suodatetaan sähköpostilinkit sekä liitteet
  - Erotetaan sisäiset ja ulkoiset postit
  - Suojataan sähköpostiliikenne domain-tasolla
    - Ilman oikeita asetuksia kuka tahansa voi esiintyä nimelläsi tai lähettää sähköpostia toimialueesi nimissä



Tiedonsuojaus ja luokittelu yrityksessä

- Miksi luokitella tietoa yrityksessä?
  - Kaikki data ei ole samanarvoista
    - Julkinen, sisäinen, luottamuksellinen, rajattu
  - Luokittelun avulla voidaan määrittää esim. tiedon salaaminen tai jakamisoikeudet.
    - Tiedon jakaminen linkkien avulla on aina riski.

- Miten?
  - Määrittele ja ota käyttöön tiedon luokittelu
  - Estä sensitiivisen tiedon lähetys (henkilötunnukset, pankkitiedot, terveystiedot)
  - Estä ulkoinen tiedon jakaminen, rajaa sisäistä jakamista.



Tilien seuranta ja logitus 365-ympäristössä

- Miksi seurata tilejä ja logittaa 365-ympäristöä?
  - Ilman lokia
    - Et tiedä mitä tapahtui
    - Et voi todistaa mitään
  - Ilman hälytyksiä
    - Et havaitse tilimurtoja tai pääkäyttäjien tunnusten väärinkäyttöjä
    - Et näe onko kyseessä sisäinen vai ulkoinen hyökkäys

- Miten?
  - Määrittele realistinen logitus päälle (180 päivää)
    - Kerää logit talteen keskitettyyn palveluun
  - Integroi tarvittaessa tietoturvapalvelua tuottavan tahon valvomoon.
  - Ota käyttöön työkalu 365 poliitikoiden valvontaa varten.

M365-ympäristön varmistus

- Miksi 365-ympäristö pitää varmistaa?
  - Microsoft vastaa vain **palvelusta**
  - Asiakas vastaa **tiedosta**
  - Tämä mahdollistaa tiedon menettämisen tahallisesti tai tahattomasti
- Miten?
  - Tiedosta mikä on kriittistä tietoa yrityksellesi.
  - Tiedosta missä tietosi sijaitsee ja mitkä ovat sen vaateet.
    - Suomi / Eurooppa / Koko maailma
  - Varmista luotettavaan sijaintiin 3. osapuolen tuotteilla.
  - Kriittinen tieto kannattaa varmistaa myös offline-medialle

Käyttäjien koulutus

- Miksi käyttäjiä pitää kouluttaa?
  - Ihminen on heikoin lenkki
    - Väsyy, luottaa tai erehtyy
  - Tietoturvakoulutus ja simuloidut hyökkäykset ovat hyvä suoja uhkia vastaan
- Miten?
  - Tee ohje käyttäjille:”Miten toimin epäilyttävässä tilanteessa?”
  - Ota käyttöön simuloidut kalasteluhyökkäykset

Hallinnollinen tietoturva

- Miksi pitää olla hallinnollista tietoturvaa?
  - Ohjeistus yritystasolla toimimiseen tietoturvan osalta
- Miten?
  - Tee ohje mitä oikeuksia käyttäjä saa osana organisaatiotasi ja mitä häneltä poistetaan työsuhteen jälkeen
  - Dokumentoi pääkäyttäjäsi sekä oleelliset sovellukset sekä niiden roolipohjaiset käyttöoikeudet
  - Katselmoi oikeudet säännöllisesti

DataEnter

KIITOS!

Kysymyksiä, kommentteja tai kertomuksia?

Toni Keränen, palvelupäällikkö

toni.keranen@dataenter.fi

+358 44 7344 330

dataenter.fi